



Lesson Plans

Optimizing Converged Cisco Networks

(Exam 642-845 ONT)

Version 2.0

Table of Contents

Course Overview	2
Section 0.1: Introduction.....	4
Section 1.1: QoS Models	5
Section 1.2: Necessity for QoS and QoS Mechanisms	6
Section 1.3: QoS Implementation Tools.....	7
Section 2.1: Necessity for IP Telephony.....	8
Section 2.2: Signaling, Conversion, and Bandwidth Planning.....	9
Section 2.3: Telephony Components and Deployment Models.....	11
Section 2.4: Voice Dial Peers	13
Section 3.1: Classification	14
Section 3.2: Marking.....	15
Section 3.3: Classification and Marking Configuration	16
Section 3.4: NBAR	17
Section 4.1: Basic Queuing.....	18
Section 4.2: Advanced Queuing	19
Section 4.3: CBWFQ and LLQ Configuration	20
Section 5.1: Tail Drop and Queue Congestion	21
Section 5.2: Random Early Detection (RED) Methods	22
Section 5.3: WRED Configuration	23
Section 6.1: Traffic Policing and Shaping	24
Section 6.2: Traffic Policing and Shaping Configuration.....	25
Section 6.3: Control Plane Policing (CoPP)	26
Section 7.1: Compression	27
Section 7.2: Link Fragmentation and Inter-Leaving (LFI).....	28
Section 8.1: VPN Overview.....	29
Section 8.2: VPN QoS Preclassification.....	30
Section 9.1: AutoQoS Overview.....	31
Section 9.2: AutoQoS VoIP.....	32
Section 9.3: AutoQoS Enterprise.....	33
Section 10.1: SDM Basics	34
Section 10.2: QoS Policy Configuration with SDM.....	35
Section 11.1: WLAN Security	36
Section 11.2: WLAN Standards and Authentication	37
Section 11.3: WLAN Management Tools	38
Section 11.4: Basic WCS and WLAN Controller Configuration	39
Section 11.5: WLAN QoS	40
Practice Exams.....	41

Course Overview

This course prepares students for Exam 642-845 ONT: Optimizing Converged Cisco Networks. It focuses on implementing effective QoS techniques for converged networks.

Module 0 – Introduction

This module introduces the students to the router simulator, which is a learning tool used to complete the simulations throughout the course.

Module 1 – QoS Overview

This module provides an overview of QoS models, the reasons for QoS and QoS mechanisms, and the tools used to implement QoS on Cisco devices.

Module 2 – Voice over IP (VoIP)

This module examines Voice over IP (VoIP). Students will become familiar with the benefits of deploying an IP telephony solution, voice signaling, conversion, and bandwidth planning. Also discussed are the components of an IP telephony network, deployment models and voice dial peers.

Module 3 – Classification and Marking

In this module students will learn concepts about using classification and marking of traffic for QoS treatments.

Module 4 – Congestion Management

This module teaches the students about congestion management using basic and advanced queuing mechanisms.

Module 5 – Congestion Avoidance

This module discusses concepts about congestion avoidance mechanisms; tail drop, Random Early Detection (RED), and Weighted Random Early Detection (WRED) methods.

Module 6 – Traffic Conditioning

This module examines the role of traffic conditioning. Concepts discussed will include traffic policing, traffic shaping, and Control Plane Policing (CoPP).

Module 7 – Link Efficiency

In this module students will learn concepts about link efficiency; compression, and Link Fragmentation and Inter-Leaving (LFI).

Module 8 – QoS for VPNs

This module discusses QoS for VPNs. It first provides an overview of using a VPN to secure IP traffic and then provides information about using VPN QoS preclassification.

Module 9 – AutoQoS

In this module students will learn the basics of using AutoQoS and configuring AutoQoS VoIP and AutoQoS Enterprise.

Module 10 – Cisco Router and Security Device Manager (SDM)

This module discusses the basic concepts about deploying SDM and configuring a QoS policy using the SDM wizard.

Module 11 – Wireless LANs (WLANs)

This module examines Wireless LANs. Topics covered include; WLAN security, WLAN standards and authentication methods, and WLAN management tools. Students will learn how to configure a basic WCS configuration and a WLAN QoS.

Practice Exams

In Practice Exams students will have the opportunity to test themselves and verify that they understand the concepts and are ready to take the certification exam.

Section 0.1: Introduction

Summary

This section introduces the student to the TestOut router simulator, which is used in most of the lab exercises throughout the course. Students will become familiar with the:

- Process to complete labs.
- Elements of the Lab Report box.
- Device console.
- Icons used to represent network devices and connections.

Before you start this course, you should have completed the following course or have equivalent networking experience:

- Cisco Exam 640-802 OR
- Cisco Exam 640-822 AND Exam 640-816

Time

About 5 minutes

Section 1.1: QoS Models

Summary

This section discusses three Quality of Service (QoS) models used to guarantee a certain level of performance to a data flow. Models discussed include:

- Best Effort
- Integrated Services (IntServ)
- Differentiated Services (DiffServ)

Optimizing Converged Cisco Networks Objectives:

- 202. Describe strategies for QoS implementations (e.g. QoS Policy, QoS Models, etc.).

Lecture Focus Questions:

- How does hard QoS reserve services for traffic flows?
- Why is the Best Effort QoS model the easiest model to implement?
- What are the drawbacks of using the Integrated Services model?
- Why is the Differentiated Services model the preferred method to provide QoS?

Time

About 20 minutes

Number of Exam Questions

9 questions

Section 1.2: Necessity for QoS and QoS Mechanisms

Summary

In this section students will learn about the necessity for using QoS and QoS mechanisms. Reasons for using QoS include:

- Lack of bandwidth
- End-to-end delay
- Jitter (variable delay)
- Packet loss

QoS mechanisms include:

- Congestion management
- Congestion avoidance
- Traffic conditioning
- Link efficiency

Optimizing Converged Cisco Networks Objectives:

- 201. Explain the necessity of QoS in converged networks (e.g., bandwidth, delay, loss, etc.).

Lecture Focus Questions:

- What are the primary reasons for using QoS?
- Why was end-to-end delay not much of a problem prior to real-time traffic?
- What causes jitter or variable delay?
- How do de-jitter buffers help to provide protection against jitter on IP phones?
- What QoS mechanisms can be used to deal with network congestion?
- What are the conditions in which tail drop occurs?
- What is the difference between *policing* and *shaping*?

Time

About 25 minutes

Number of Exam Questions

14 questions

Section 1.3: QoS Implementation Tools

Summary

This section examines different tools available when implementing QoS on Cisco devices:

- Legacy CLI
- Modular QoS Command Line Interface (MQC)
- AutoQoS
- Cisco Router and Security Device Manager (SDM)

Optimizing Converged Cisco Networks Objectives:

- 202. Describe strategies for QoS implementations (e.g. QoS Policy, QoS Models, etc.).

Lecture Focus Questions:

- What are the main issues with using the Legacy CLI when configuring QoS policies?
- How does the MQC prevent QoS policy misconfigurations?
- How can you change a QoS policy which was originally generated via the SDM?
- Why is AutoQoS usually considered the fastest method for implementing a QoS solution?

Time

About 10 minutes

Number of Exam Questions

1 question

Section 2.1: Necessity for IP Telephony

Summary

This section provides information about using IP telephony. The benefits of deploying an IP telephony solution include:

- Efficient use of bandwidth.
- Lower transmission cost.
- Consolidated network expenses.
- Improved employee productivity.
- Increased management efficiency.
- Access to new communications devices.

Optimizing Converged Cisco Networks Objectives:

- 101. Describe the functions and operations of a VoIP network (e.g., packetization, bandwidth considerations, CAC, etc.).

Lecture Focus Questions:

- How does an IP telephony solution save on transmission costs?
- What is the main benefit of centralized network management for both the voice and data infrastructure?

Time

About 5 minutes

Number of Exam Questions

1 question

Section 2.2: Signaling, Conversion, and Bandwidth Planning

Summary

This section discusses voice signaling, conversion and planning the bandwidth for converged networks. Concepts covered include:

- Steps to convert an analog signal into digital form:
 - Sampling
 - Quantization
 - Encoding
 - Compression
- Considerations when calculating bandwidth requirements:
 - Packet rate
 - Packetization size
 - IP overhead
 - Data link overhead
 - Tunneling
 - MPLS or PPPoE
- Comparison of bandwidth required for G.711 and G.729 codecs depending upon the Layer 2 headers.

Optimizing Converged Cisco Networks Objectives:

- 101. Describe the functions and operations of a VoIP network (e.g., packetization, bandwidth consideration, CAC, etc.).

Lecture Focus Questions:

- What are the steps used to convert an analog signal into a digital signal? Which step is optional?
- How is a Pulse Amplitude Modulation (PAM) signal created?
- How does the Nyquist Theorem affect the sampling rate?
- What is the difference between linear quantization and logarithmic quantization?
- Why is a G.729 packet so much smaller than a G.711 packet?
- How does the bandwidth required for the voice data when using the G.711 codec compare to the bandwidth required when using the G.729 codec?
- What is the difference between voice encapsulation using G.711 and voice encapsulation using G.729?
- Which layer 2 frame header adds the most bytes? Which adds the least amount of bytes?
- What components do you add to calculate the bandwidth for a single call?
- How does VAD save bandwidth, and how much is saved?

Time

About 35 minutes

Number of Exam Questions

10 questions

Section 2.3: Telephony Components and Deployment Models

Summary

This section examines components of telephony and deployment models. Concepts covered include:

- Major components of an IP telephony network:
 - IP phone
 - Call agent
 - Voice gateway
 - Gatekeeper
 - Multipoint Control Unit (MCU)
- Voice gateway interface types:
 - Analog interfaces
 - Digital interfaces
- Telephony deployment models:
 - Single site
 - Multisite with centralized call processing
 - Multisite with distributed call processing
 - Clustering over the WAN

Optimizing Converged Cisco Networks Objectives:

- 101. Describe the functions and operations of a VoIP network (e.g., packetization, bandwidth considerations, CAC, etc.).
- 102. Describe and identify basic voice components in an enterprise network (e.g. Gatekeepers, Gateways, etc.)

Lecture Focus Questions:

- On what device is a voice gateway implemented?
- How does a gatekeeper provide scalability to a VoIP deployment?
- How does CAC ensure the quality of existing voice sessions?
- What are the functions of the call agent in an IP telephony network?
- What are other names for the call agent?
- What is the function of a MCU?
- What is the major difference between the *multisite with centralized call processing* deployment model and the *multisite with distributed call processing* deployment model?
- What feature provides fallback calling functionality when a remote site loses its WAN connection?
- What types of interfaces provide connections for analog phones, fax machines, or a PSTN?

Time

About 35 minutes

Number of Exam Questions

10 questions

Section 2.4: Voice Dial Peers

Summary

This section discusses the basic configuration requirements of voice dial peers and the commands to configure voice dial peers.

Students will learn how to:

- Configure Cisco routers as voice gateways by defining the FXS port for a local analog connection.
- Configure the POTS and VoIP destination patterns for VoIP communication.

Optimizing Converged Cisco Networks Objectives:

- 102. Describe and identify basic voice components in an enterprise network (e.g., Gatekeepers, Gateways, etc.).

Lecture Focus Questions:

- How does the voice dial peer configuration provide connectivity to phones remotely located without the use of a CallManager?
- What function does the FXS port provide to an analog device in a voice dial peers model?
- How does the Real-time Transport Protocol (RTP) session participate in a voice dial peers model?

Time

About 30 minutes

Lab/Activity

- Configure Voice Dial Peers

Number of Exam Questions

2 questions

Section 3.1: Classification

Summary

In this section students will explore using classification to identify types of traffic for QoS treatments to provide a predictable level of service.

Optimizing Converged Cisco Networks Objectives:

- 301. Describe classification and marking (e.g., CoS, ToS, IP Precedence, DSCP, etc.).

Lecture Focus Questions:

- What types of classification options can be used to classify and match incoming data?
- Why is the VoIP traffic class given the highest priority?
- What is the main difference between the *voice applications* traffic class and the *mission critical* traffic class?
- Where should traffic classification occur?

Time

About 8 minutes

Number of Exam Questions

18 questions

Section 3.2: Marking

Summary

This section discusses using marking to tag a packet to identify and distinguish it from other packets during QoS treatment. Concepts covered include:

- The role of Layer 2 markings
- The role of Layer 3 markings
- Corresponding Layer 2 and Layer 3 markings
- The role of the trust boundary

Optimizing Converged Cisco Networks Objectives:

- 301. Describe classification and marking (e.g., CoS, ToS, IP Precedence, DSCP, etc.).

Lecture Focus Questions:

- What makes Layer 3 markings more valuable than Layer 2 markings?
- How many values does the CoS and EXP fields generate that can be used to categorize data?
- Which bits in the ToS byte were named the Differentiated Service Code Point, or DSCP?
- What are the major differences and similarities between the IPP and DSCP markings?
- How does DSCP provide backwards compatibility to IPP-based systems?
- What is the binary value for the Expedited Forwarding (EF) DSCP marking?
- What establishes a trust boundary?
- What types of values are checked at the trust boundary?
- What is a QoS domain?

Time

About 25 minutes

Number of Exam Questions

2 questions

Section 3.3: Classification and Marking Configuration

Summary

This section examines implementing classification and marking. Concepts covered include:

- Basic steps in MQC to implement classification and marking.
- Commands used to classify and mark traffic.

Students will learn to:

- Create a class map to identify specific types of marked traffic.
- Create a policy map to indicate the actions applied to each class.
- Apply the policy map to an interface.

Optimizing Converged Cisco Networks Objectives:

- 301. Describe classification and marking (e.g., CoS, ToS, IP Precedence, DSCP, etc.).

Lecture Focus Questions:

- What are the three basic steps to implementing classification and marking?
- What is the effect of using the *match-all* keyword and the *match-any* keyword when creating a class map?
- How do you apply the service policy to the specified interface?
- How do you apply a service policy within a class?

Time

About 30 minutes

Lab/Activity

- Configure Classification and Marking
- Find Classification and Marking Information

Number of Exam Questions

2 questions

Section 3.4: NBAR

Summary

In this section students will learn about using Network Based Application Recognition (NBAR) to provide intelligent data classification on Layer 4-7 information. Concepts covered include:

- The role of NBAR.
- Application types that NBAR can recognize and classify.
- The role of subport classification.
- NBAR limitations.
- Commands used to enable NBAR.

Students will learn to:

- Configure NBAR to identify VoIP traffic and then mark the VoIP traffic.
- Configure NBAR to identify file-sharing traffic and then drop the traffic.

Optimizing Converged Cisco Networks Objectives:

- 302. Describe and configure NBAR for classification.

Lecture Focus Questions:

- How does NBAR identify specific types of traffic?
- What are the functions of *subport classification*?
- How can PDLMs help NBAR?
- What type of information does the NBAR Protocol Discovery feature provide?

Time

About 45 minutes

Lab/Activity

- Configure NBAR 1
- Configure NBAR 2
- Find NBAR Classification and Marking Information

Number of Exam Questions

8 questions

Section 4.1: Basic Queuing

Summary

This section examines using basic queuing to sort and prioritize traffic. Concepts covered include:

- Congestion management
- Basic queuing mechanisms:
 - First in, First out (FIFO)
 - Priority Queuing (PQ)
 - Round Robin and Weighted Round Robin (WRR)
 - Custom Queuing (CQ)

Optimizing Converged Cisco Networks Objectives:

- 303. Explain congestion management and avoidance mechanisms (e.g., FIFO, PQ, WRR, WRED, etc.).

Lecture Focus Questions:

- What are the major causes of interface congestion?
- What is a congestion management mechanism?
- What is the difference between Round Robin and Weighted Round Robin?
- How does starvation of a queue occur when using Priority Queuing?
- What are the differences between Custom Queuing and Priority Queuing?

Time

About 15 minutes

Number of Exam Questions

3 questions

Section 4.2: Advanced Queuing

Summary

In this section students will learn about the following advanced queuing methods:

- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)

Optimizing Converged Cisco Networks Objectives:

- 303. Explain congestion management and avoidance mechanisms (e.g., FIFO, PQ, WRR, WRED, etc.).

Lecture Focus Questions:

- How does Weighted Fair Queuing (WFQ) determine how packets should be classified and queued?
- What does the hold queue represent?
- What types of packet information are used to identify *traffic flows*?
- What does the Congestive Discard Threshold (CDT) define and how is the CDT affected according to the number of queues?
- How does Class-Based Weighted Fair Queuing (CBWFQ) improve on WFQ?
- What types of user-defined criteria does CBWFQ allow when sorting traffic into different classes?
- When using CBWFQ, what is the total reservable limit of the interface's available bandwidth?
- What function does Low Latency Queuing (LLQ) provide?

Time

About 20 minutes

Number of Exam Questions

3 questions

Section 4.3: CBWFQ and LLQ Configuration

Summary

This section discusses commands used to configure CBWFQ and LLQ.

Students will learn how to:

- Implement Class-Based Weighted Fair Queuing (CBWFQ) by specifying percentages of bandwidth for specific traffic classes.
- Implement Low Latency Queuing (LLQ) for real-time traffic.
- Implement Weighted Fair Queuing (WFQ) to the class-default class.

Optimizing Converged Cisco Networks Objectives:

- 303. Explain congestion management and avoidance mechanisms (e.g., FIFO, PQ, WRR, WRED, etc.).

Lecture Focus Questions:

- What command creates a Low Latency Queuing (LLQ)?
- Within which class can Weighted Fair Queuing (WFQ) be applied?
- In which direction is a congestion management QoS policy applied?

Time

About 25 minutes

Lab/Activity

- Configure CBWFQ
- Configure LLQ

Number of Exam Questions

3 questions

Section 5.1: Tail Drop and Queue Congestion

Summary

In this section students will learn the basics of how Cisco routers use tail drop to avoid queue congestion.

Optimizing Converged Cisco Networks Objectives:

- 303. Explain congestion management and avoidance mechanisms (e.g., FIFO, PQ, WRR, WRED, etc.).

Lecture Focus Questions:

- When does tail drop occur? How is it implemented?
- What is the function of TCP *slow-start*?
- What happens to packets already in the queue during periods of congestion?
- How is TCP global-synchronization related to slow-start?

Time

About 5 minutes

Section 5.2: Random Early Detection (RED) Methods

Summary

This section provides an overview of Random Early Detection (RED) methods used to avoid a queue filling up. Details about the following methods are presented:

- Random Early Detection (RED)
- Weighted Random Early Detection (WRED)

Optimizing Converged Cisco Networks Objectives:

- 303. Explain congestion management and avoidance mechanisms (e.g., FIFO, PQ, WRR, WRED, etc.).

Lecture Focus Questions:

- What are the major differences between Random Early Detection (RED) and Weighted Random Early Detection (WRED)?
- What are the parameters used to define a packet's drop-probability?
- When is the *Mark Probability Denominator* enabled?
- Which type of congestion management queuing cannot use WRED?

Time

About 10 minutes

Number of Exam Questions

3 questions

Section 5.3: WRED Configuration

Summary

This section discusses commands used to configure WRED modes.

Students will learn how to:

- Configure WRED within an existing service policy.
- Configure WRED to use the DSCP value of a packet.
- Customize WRED by setting the minimum threshold, the maximum threshold, and the mark probability denominator.

Optimizing Converged Cisco Networks Objectives:

- 303. Explain congestion management and avoidance mechanisms (e.g., FIFO, PQ, WRR, WRED, etc.).

Lecture Focus Questions:

- What DiffServ values are used by default when enabling WRED?
- What DSCP settings are available when configuring WRED to use the DSCP value of a packet?

Time

About 20 minutes

Lab/Activity

- Configure WRED 1
- Configure WRED 2

Number of Exam Questions

1 question

Section 6.1: Traffic Policing and Shaping

Summary

This section discusses details about traffic policing and shaping. Concepts covered include:

- Traffic policing characteristics.
- The manner in which traffic policing operates.
- The role of traffic shaping.
- The manner in which traffic shaping operates.

Optimizing Converged Cisco Networks Objectives:

- 304. Describe traffic policing and traffic shaping (i.e., traffic conditioners).

Lecture Focus Questions:

- What is the difference between *traffic policing* and *traffic shaping*?
- How is the Committed Time Interval (Tc) calculated for traffic policing?
- What is *sub-rate access*?
- How is *conforming traffic* different from *exceeding traffic*?
- Why is *average shaping* the best option for voice traffic when using up unused bandwidth?

Time

About 35 minutes

Number of Exam Questions

6 questions

Section 6.2: Traffic Policing and Shaping Configuration

Summary

This section discusses commands used to configure traffic policing and shaping.

Students will learn how to:

- Configure traffic policing to restrict traffic on a class to a specified rate.
- Configure how traffic will be handled when bursting above the contracted rate or bursting above the excess burst rate.
- Configure traffic shaping with the average or peak option.

Optimizing Converged Cisco Networks Objectives:

- 304. Describe traffic policing and traffic shaping (i.e., traffic conditioners).

Time

About 25 minutes

Lab/Activity

- Configure Policing
- Configure Shaping

Number of Exam Questions

2 questions

Section 6.3: Control Plane Policing (CoPP)

Summary

This section explores concepts about using Control Plane Policing (CoPP) to prevent DoS attacks. Concepts covered include:

- Problems that may occur to a switch or router during a DoS attack.
- The role of CoPP.
- Steps to configure CoPP.
- Commands to configure CoPP.

Students will learn how to:

- Configure CoPP for IP addresses and for specific application traffic.

Optimizing Converged Cisco Networks Objectives:

- 305. Describe Control Plane Policing.

Lecture Focus Questions:

- How does Control Plane Policing (CoPP) prevent Denial of Service (DoS) attacks?
- What types of problems might indicate that a switch or router is under a DoS attack?
- What type of traffic is handled by the *data* plane in the router?
- What type of traffic is handled by the *control* or *management* planes in the router?

Time

About 25 minutes

Lab/Activity

- Configure CoPP

Number of Exam Questions

8 questions

Section 7.1: Compression

Summary

This section examines using compression to avoid serialization delay. Concepts covered include:

- Compression methods:
 - Payload
 - Header
- Commands used to configure compression

Students will learn how to:

- Configure RTP header compression.

Optimizing Converged Cisco Networks Objectives:

- 306. Describe WAN link efficiency mechanisms (e.g., Payload/Header Compression, MLP with interleaving, etc.).

Lecture Focus Questions:

- When using payload compression, why would you select hardware compression over software compression?
- What is difference in how the compression is performed for header versus payload compression?
- When using payload compression, what software payload compression techniques are available for Cisco's internetworking devices?
- Why is header compression suitable for VoIP applications?
- At what link speed should header compression be implemented?

Time

About 30 minutes

Lab/Activity

- Configure RTP Header Compression

Number of Exam Questions

5 questions

Section 7.2: Link Fragmentation and Inter-Leaving (LFI)

Summary

This section provides information about using Link Fragmentation and Inter-Leaving (LFI) to avoid queuing delays. Concepts covered include:

- The role of LFI.
- Commands to enable LFI.

Optimizing Converged Cisco Networks Objectives:

- 306. Describe WAN link efficiency mechanisms (e.g., Payload/Header Compression, MLP with interleaving, etc.).

Lecture Focus Questions:

- How does LFI implementation avoid queuing delays?
- Why is LFI typically implemented on WAN links with speeds below 768 kbps?
- What LFI methods are available?

Time

About 10 minutes

Number of Exam Questions

4 questions

Section 8.1: VPN Overview

Summary

This section provides an overview of using Virtual Private Network (VPN) to secure IP traffic. Concepts covered include:

- The role of a VPN
- VPN protocol types:
 - General Routing Encapsulation (GRE)
 - Internet Protocol Security ((IPsec)

Optimizing Converged Cisco Networks Objectives:

- 307. Describe and configure QoS Pre-Classify.

Lecture Focus Questions:

- In a VPN, how do the routers identify where to deliver the packet to the destination device?
- How can GRE provide secure tunneling?
- What are the main differences between GRE and IPsec, and which is the most widely deployed?
- What benefits are provided by VPNs using IPsec?
- How do the two IPsec modes of operation differ?

Time

About 10 minutes

Number of Exam Questions

2 questions

Section 8.2: VPN QoS Preclassification

Summary

This section provides an overview of using QoS preclassification. Concepts covered include:

- VPN traffic without QoS preclassification.
- VPN traffic with QoS.
- Commands used to configure QoS preclassification.

Optimizing Converged Cisco Networks Objectives:

- 307. Describe and configure QoS Pre-Classify.

Lecture Focus Questions:

- What is the purpose of QoS Preclassification?
- What type of information is included in an inner (pre-tunnel) header?
- Which types of scenarios require the use of QoS Preclassification for end-to-end QoS?
- Where do you apply QoS Preclassification for a VPN that uses IPsec or a VPN that uses tunnel interfaces?

Time

About 25 minutes

Number of Exam Questions

8 questions

Section 9.1: AutoQoS Overview

Summary

This section provides an overview of using the AutoQoS feature to simplify the deployment of existing QoS features. Concepts covered include:

- The role of AutoQoS.
- AutoQoS prerequisites.

Optimizing Converged Cisco Networks Objectives:

- 401. Explain the functions and operations of AutoQoS.

Lecture Focus Questions:

- What are the advantages of using AutoQoS?
- What tool provides the network traffic discovery results which are used by AutoQoS?
- What prerequisites should be satisfied before AutoQoS is enabled on a router?
- How could an inaccurately-configured interface bandwidth affect AutoQoS?
- What step must you take if the bandwidth is changed after an AutoQoS implementation?

Time

About 12 minutes

Section 9.2: AutoQoS VoIP

Summary

In this section students will learn about configuring AutoQoS VoIP. Concepts covered include:

- Implementing and managing an AutoQoS VoIP configuration.
- Commands to configure and verify AutoQoS VoIP.

Students will learn how to:

- Enable AutoQoS VoIP on switch interfaces connected to IP phones.
- Enable AutoQoS VoIP on a router interface to trust DSCP settings.

Optimizing Converged Cisco Networks Objectives:

- 401. Explain the functions and operations of AutoQoS.
- 403. Configure, verify, and troubleshoot AutoQoS implementations (i.e., MQC).

Lecture Focus Questions:

- How would you modify an AutoQoS VoIP configuration?
- What types of devices work with AutoQoS VoIP?
- How will disabling CDP on a switch affect AutoQoS VoIP configurations?

Time

About 35 minutes

Lab/Activity

- Configure AutoQoS VoIP 1
- Configure AutoQoS VoIP 2
- Find AutoQoS VoIP Information

Number of Exam Questions

3 questions

Section 9.3: AutoQoS Enterprise

Summary

This section examines details about AutoQoS Enterprise. Concepts covered include:

- Deployment stages for AutoQoS Enterprise:
 - Discovery
 - Policy Generation and Implementation
- Commands to configure and verify AutoQoS Enterprise

Students will learn how to:

- Implement AutoQoS Discovery on a serial interface using NBAR or DSCP markings.
- Display the discovery results before they are implemented on the interface.
- Implement the AutoQoS policy proposal for the interface.
- Display the AutoQoS templates and initial configuration.

Optimizing Converged Cisco Networks Objectives:

- 401. Explain the functions and operations of AutoQoS.
- 403. Configure, verify, and troubleshoot AutoQoS implementations (i.e., MQC).

Lecture Focus Questions:

- What are the deployment stages of AutoQoS Enterprise?
- When is NBAR support automatically loaded into memory?
- What types of QoS mechanisms will AutoQoS-generated policies recommend for implementation on slow WAN links running less than or equal to 768 kbps?
- When can you fine-tune AutoQoS policies, and what tool do you use?

Time

About 40 minutes

Lab/Activity

- Configure AutoQoS Enterprise
- Find AutoQoS Enterprise Information

Number of Exam Questions

9 questions

Section 10.1: SDM Basics

Summary

This section discusses the basics of implementing the Cisco Router and Security Device Manager (SDM) to manage Cisco routers. Concepts covered include:

- Deploying the SDM
- Viewing SDM information
- SDM prerequisites

Optimizing Converged Cisco Networks Objectives:

- 402. Describe the SDM QoS Wizard.

Lecture Focus Questions:

- What types of wizards are available within the Cisco Router and Security Device Manager (SDM)?
- What privilege level is necessary to log in to the SDM and make configuration changes?

Time

About 15 minutes

Number of Exam Questions

1 question

Section 10.2: QoS Policy Configuration with SDM

Summary

This section explores configuring a QoS policy with the SDM wizard.

Students will learn how to:

- Configure a QoS policy using the SDM wizard.
- Use the SDM to verify a router's running-config QoS policies.

Optimizing Converged Cisco Networks Objectives:

- 402. Describe the SDM QoS Wizard.

Lecture Focus Questions:

- What are the advantages of using the SDM wizard to create a QoS configuration?
- How do you create bandwidth allocations using SDM?
- What are the two main types of traffic classes that SDM will create for a QoS policy?
- What is the maximum percentage of bandwidth that can be allocated for a single QoS policy?
- In what direction can you create and apply QoS policies when using the QoS SDM wizard?
- In which SDM locations can you view the configurations after you have created the QoS policies, and which location will allow you to edit the QoS configuration?

Time

About 30 minutes

Lab/Activity

- Configure QoS with SDM.
- Find QoS information with SDM..

Number of Exam Questions

5 questions

Section 11.1: WLAN Security

Summary

In this section students will learn the basics of securing a wireless network. Concepts covered include:

- Key risks associated with wireless networks.
- Methods to address security issues:
 - Change SSID from defaults
 - Enable MAC address filtering
 - Encryption
- Security goals to protect a network

Optimizing Converged Cisco Networks Objectives:

- 501. Describe and configure wireless security on Cisco Clients and APs (e.g., SSID, WEP, LEAP, etc.).

Lecture Focus Questions:

- What are the key risks associated with wireless networks?
- What are the primary security goals to protect a network system?
- Why is it important to change the SSID from the defaults?
- What are the advantages of configuring a MAC address filtering system?

Time

About 10 minutes

Number of Exam Questions

1 question

Section 11.2: WLAN Standards and Authentication

Summary

This section provides an overview of WLAN standards and authentication methods. Concepts covered include:

- Standards that provide security for wireless networks:
 - Wired Equivalent Privacy (WEP)
 - Wi-Fi Protected Access (WPA)
 - Wi-Fi Protected Access 2 (WPA2) or 802.11i
- Authentication methods on a wireless network:
 - Open
 - Shared secret
 - 802.1x
- 802.1x authentication protocol types:
 - 802.1x Extensible Authentication Protocol (EAP)
 - Lightweight EAP (LEAP)
 - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
 - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)
 - Protected EAP (PEAP)

Optimizing Converged Cisco Networks Objectives:

- 501. Describe and configure wireless security on Cisco Clients and APs (e.g., SSID, WEP, LEAP, etc.).

Lecture Focus Questions:

- What are the major security standards for wireless networks?
- What are the weaknesses in WEP for securing a wireless network?
- What makes WPA2 more secure than WPA?
- How does EAP-Fast protect the client's credentials as they are exchanged?
- Why is EAP-TLS considered one of the strongest EAP solutions?

Time

About 35 minutes

Number of Exam Questions

10 questions

Section 11.3: WLAN Management Tools

Summary

This section discusses using WLAN management tools. Concepts covered include:

- Cisco WLAN implementation methods:
 - Autonomous
 - Lightweight
- CiscoWorks Wireless LAN Solution Engine (WLSE)
- Wireless Domain Services (WDS)
- Cisco Wireless Control System (WCS)
- WCS versions:
 - WCS Base
 - WCS with Location
 - WCS with Location plus 2700 Series Appliance

Optimizing Converged Cisco Networks Objectives:

- 502. Describe basic wireless management (e.g., WLSE and WCS). Configure and verify basic WCS configuration (i.e., login, add/review controller/AP status, security, and import/review maps).

Lecture Focus Questions:

- What are the major differences between an autonomous and a lightweight WLAN implementation method?
- What devices are used in the autonomous and lightweight WLAN implementation methods?
- How does the Wireless LAN Solution Engine (WLSE) centrally manage autonomous access points?
- What function does the Wireless Domain Services (WDS) provide?
- What is the advantage of using WCS over WLSE?
- What is the difference between the features available with the *WCS with Location* version and the *WCS with location plus 2700 Series Appliance* version?

Time

About 35 minutes

Number of Exam Questions

18 questions

Section 11.4: Basic WCS and WLAN Controller Configuration

Summary

This section explores configuring a basic WCS and WLAN controller to manage a wireless network.

Students will learn how to:

- Add an existing WLAN controller into the WCS and verify that the access points imported correctly.

Optimizing Converged Cisco Networks Objectives:

- 502. Describe basic wireless management (e.g., WLSE and WCS). Configure and verify basic WCS configuration (i.e., login, add/review controller/AP status, security, and import/review maps).

Lecture Focus Questions:

- What are the alarm color codes for WCS?
- Which WCS menu configures the communication with a Location Appliance?
- How can you add and manage access points in the WCS?
- What CLI command reboots the WLAN Controller?

Time

About 30 minutes

Lab/Activity

- Associate WLAN Controllers with WCS

Number of Exam Questions

13 questions

Section 11.5: WLAN QoS

Summary

In this section students will learn the basics of WLAN QoS. Concepts covered include:

- Enhanced DCF (EDCF)
- Wi-Fi Multimedia (WMM)
- WMM and 802.11e priority levels:
 - Platinum
 - Gold
 - Silver
 - Bronze
- Tools to configure WLAN QoS:
 - WLAN Controller
 - Wireless Control System (WCS)

Students will learn how to:

- On the WCS, configure the QoS profile settings for the controller(s) to provide QoS support.

Optimizing Converged Cisco Networks Objectives:

- 503. Describe and configure WLAN QoS.

Lecture Focus Questions:

- How can you provide QoS to devices that use CSMA/CA?
- How can you manage the use of the airwaves and give certain devices priority treatment?
- How do you provide end-to-end QoS while crossing wired to wireless boundaries?
- How do the WMM and 802.11e priority levels correspond to each other?

Time

About 10 minutes

Lab/Activity

- Configure WLAN QoS with WCS

Number of Exam Questions

12 questions

Practice Exams

Summary

This section provides information to help prepare students to take the exam and to register for the exam.

Students will also have the opportunity of testing their mastery of the concepts presented in this course to reaffirm that they are ready for the certification exam. For example, all questions that apply to **Objective 100. Describe Cisco VoIP implementations** are grouped together and presented in practice exam **100. Describe Cisco VoIP implementations, All Questions**. Students will typically take about 60-90 minutes to complete each of the following practice exams.

100. Describe Cisco VoIP implementations, All Questions (26 questions)

200. Describe QoS considerations, All Questions (23 questions)

300. Describe DiffServ QoS implementations, All Questions (79 questions)

400. Implement AutoQoS, All Questions (21 questions)

500. Implement WLAN security and management, All Questions (54 questions)

The *Certification Practice Exam* consists of 55 questions that are randomly selected from the above practice exams. Each time the Certification Practice Exam is accessed different questions may be presented. The Certification Practice Exam has a time limit of 90 minutes -- just like the real certification exam. A passing score of 95% should verify that the student has mastered the concepts and is ready to take the real certification exam.